

**IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF GEORGIA  
ATLANTA DIVISION**

GLORIA BRUNSON, KEVIN  
DAHLBERG, JAMAL DOUGLAS,  
and EARL YOUNG, individually and  
on behalf of all others similarly  
situated,

Plaintiffs,

v.

THE HOME DEPOT, INC., Delaware  
Corporation, and JOHN DOE,

Defendants.

Case No.

**COMPLAINT - CLASS ACTION  
AND DEMAND FOR JURY TRIAL**

Plaintiffs Gloria Brunson, Kevin Dahlberg, Jamal Douglas, and Earl Young bring this Class Action Complaint and Demand for Jury Trial (“Complaint”) against Defendants The Home Depot, Inc. (“Home Depot”) and John Doe for violating the Illinois Biometric Information Privacy Act, 740 ILCS 14/1 *et seq.* (“BIPA”). Plaintiffs allege the following upon personal knowledge as to themselves and their own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by their attorneys:

## **NATURE OF THE ACTION**

1. Home Depot is the country's largest home-improvement retailer, with more than 2,200 stores generating over \$108 billion in annual revenue.

2. Of those 2,200-plus stores, 76 are located in Illinois, where it has been illegal since 2008 to collect an individual's biometric information or identifier—such as a fingerprint, voiceprint, or faceprint—without the individual's informed, written consent. 740 ILCS 14/15(b).

3. Despite the decade-old prohibition on collecting biometric data without consent, Home Depot has augmented its in-store security cameras with software that track individuals' movements throughout the store using a unique scan of face geometry. Put simply, Defendants surreptitiously attempt to collect the faceprint of every person who appears in front of one of their facial-recognition cameras.

4. Defendants actively conceal their faceprinting practices from the public. When reporters have inquired about Home Depot's use of facial recognition, it has refused comment, and when privacy-minded customers consult the Privacy and Security Statement on [www.homedepot.com](http://www.homedepot.com), they find no mention whatsoever of biometric information or faceprint collection.

5. Defendants' systemic and covert privacy intrusion is plainly unlawful in Illinois.

6. Plaintiffs bring this Complaint seeking an order (i) declaring that Defendants' conduct violates BIPA, (ii) requiring that Defendants cease the unlawful activities described herein and destroy the biometric data they unlawfully collected, and (iii) awarding Plaintiffs and the Class statutory damages of \$5,000 per violation, plus their attorneys' fees and costs.

### **PARTIES**

7. Plaintiff Brunson is a natural person and citizen of the State of Illinois.

8. Plaintiff Dahlberg is a natural person and a citizen of the State of Illinois.

9. Plaintiff Douglas is a natural person and a citizen of the State of Illinois.

10. Plaintiff Young is a natural person and a citizen of the State of Illinois.

11. Defendant Home Depot is a corporation organized under the laws of the State of Delaware, with its headquarters and principal place of business located

at 2455 Paces Ferry Rd. NW, Atlanta, Georgia 30339. Home Depot conducts business throughout this District, and the State of Georgia.

12. Defendant John Doe is the vendor and operator of the facial-recognition system used by Home Depot. Doe's citizenship is unknown to Plaintiffs.

### **JURISDICTION AND VENUE**

13. This Court has jurisdiction over the subject-matter of this action pursuant to 28 U.S.C. § 1332(d) because all Plaintiffs are citizens of a state different from at least one Defendant, and because Plaintiffs and the Class seek more than \$5,000,000 in damages.

14. This Court has personal jurisdiction over Home Depot because it is headquartered in Georgia.

15. This Court has personal jurisdiction over Defendant Doe because it because it conducts business in Georgia and it contracted with Home Depot in Georgia to provide facial-recognition services.

16. Venue is proper in this District under 28 U.S.C. § 1391(b) because Home Depot resides in this District.

## COMMON FACTUAL ALLEGATIONS

### *The Biometric Information Privacy Act*

17. Illinois enacted BIPA in 2008.

18. BIPA regulates two types of biometric data. First, BIPA regulates any “biometric identifier,” which means “a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry,” and specifically excludes a lengthy list of identifiers outside that scope. 740 ILCS 14/10. Second, it regulates any “biometric information,” which “means any information, regardless of how it is captured, converted, stored, or shared, based on an individual’s biometric identifier used to identify an individual.” *Id.* Biometric information “does not include information derived from items or procedures excluded under the definition of biometric identifiers.” *Id.*

19. BIPA regulates the entire lifecycle of biometric data, from capture and collection to use and disclosure.

20. As to the origination of biometric data, BIPA provides that “[n]o private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person’s or a customer’s biometric identifier or biometric information, unless it first: (1) informs the subject or the subject’s legally authorized

representative in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative."

21. BIPA likewise restricts the disclosure of biometric data, providing that "[n]o private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless: (1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure; (2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or biometric information or the subject's legally authorized representative; (3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or (4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction." 740 ILCS 14/15(d).

22. When it comes to exploiting biometric data, BIPA creates even stricter proscriptions. Reflecting an intent to preclude the formation of a market for biometric data, BIPA provides without exception that “[n]o private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person’s or a customer’s biometric identifier or biometric information.” 740 ILCS 14/15/(c).

23. To facilitate the informed notice and consent provisions described above, BIPA also requires that any private entity in possession of biometric identifiers or information must publish a written policy “establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual’s last interaction with the private entity, whichever occurs first.” 740 ILCS 14/15(a).

24. Finally, BIPA requires that any entity possessing biometric identifiers or information “(1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity’s industry; and (2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or

more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.” 740 ILCS 14/15(e).

25. BIPA also includes a private right of action authorizing “[a]ny person aggrieved by a violation of” the statute to sue and recover for each violation liquidated damages of \$1,000, or \$5,000 in the event of an intentional or reckless violation, plus attorneys’ fees, costs, and appropriate injunctive relief. 740 ILCS 14/20.

***Defendants’ Wanton Disregard for Customer Privacy***

26. Defendants operate a sweeping surveillance system with facial recognition at its core but disregard BIPA in its entirety.

27. In-store facial recognition systems work by scanning video footage of a person’s face for certain geometric points, such as the distance between the eyes, nose, and ears, among others. Those data points are then reflected in a data string reflecting the individual’s faceprint.

28. As the customer moves through a store and is detected by cameras, the facial-recognition technology repeatedly re-maps the customer’s facial geometry, and compares it against the stored faceprint, all while tracking the individual’s movement throughout the store.

29. Framed as a loss-prevention measure, these systems allow stores to follow customers, to identify particular individuals when they enter the store and, in some cases, to track shoppers across multiple stores and identify “suspicious” shopping activity.

30. Although it has steadfastly refused comment when asked about its facial-recognition practices, Home Depot has in fact integrated facial-recognition software into its security camera system.

31. Defendants begin tracking customers as soon as they enter Home Depot stores. Home Depot’s security cameras and its checkout cameras operate on a connected system, with facial-recognition technology running on the footage obtained. As the customer walks through the store and makes their way toward checkout, the facial-recognition software tracks their every movement, through and beyond their purchase.

32. Despite BIPA’s clear edict, Defendants do not provide a publicly available biometric-data retention schedule, nor do they obtain Home Depot customers’ informed, written consent prior to the collection, use, and disclosure of their biometric identifiers.

### **FACTUAL ALLEGATIONS SPECIFIC TO PLAINTIFF BRUNSON**

33. Plaintiff Brunson made purchases at an Illinois Home Depot in August 2018, December 2018, and June 2019.

34. On each occasion Plaintiff Brunson entered a Home Depot store, she was repeatedly viewed by Home Depot's security cameras, which captured and collected Plaintiff Brunson's faceprint. In fact, Home Depot has collected a new faceprint from Plaintiff Brunson each time she appeared on a different security camera, meaning several times per store visit.

35. Home Depot shared the security camera footage and Plaintiff Brunson's faceprint with Defendant Doe.

36. Defendants do not provide a publicly available retention schedule specifying the period for which they will retain Plaintiff Brunson's faceprint.

37. Defendants have never informed Plaintiff Brunson of the purpose for which they were capturing or collecting her faceprint or the duration for which they would retain it, nor did Defendants receive a written release from Plaintiff Brunson authorizing the collection.

38. Because she was never informed of the collection of her faceprint, Plaintiff Brunson did not consent to the capture or collection of her faceprint.

39. Plaintiff Brunson was injured as a result of the violation of her legally protected right not to have her faceprint collected without consent.

**FACTUAL ALLEGATIONS SPECIFIC TO PLAINTIFF DAHLBERG**

40. Plaintiff Dahlberg is a contractor and handyman, and he has made purchases at Home Depot stores in Illinois at least ten times in the last year.

41. On each occasion Plaintiff Dahlberg entered a Home Depot store, he was repeatedly viewed by Home Depot's security cameras, which captured and collected Plaintiff Dahlberg's faceprint. In fact, Home Depot has collected a new faceprint from Plaintiff Dahlberg each time he appeared on a different security camera, meaning several times per store visit.

42. Home Depot shared the security-camera footage and Plaintiff Dahlberg's faceprint with Defendant Doe.

43. Defendants do not provide a publicly available retention schedule specifying the period for which they will retain Plaintiff Dahlberg's faceprint.

44. Defendants have never informed Plaintiff Dahlberg of the purpose for which they were capturing or collecting his faceprint or the duration for which they would retain it, nor did Defendants receive a written release from Plaintiff Dahlberg authorizing the collection.

45. Because he was never informed of the collection of his faceprint, Plaintiff Dahlberg did not consent to the capture or collection of his faceprint.

46. Plaintiff Dahlberg was injured as a result of the violation of his legally protected right not to have his faceprint collected without consent.

**FACTUAL ALLEGATIONS SPECIFIC TO PLAINTIFF DOUGLAS**

47. Plaintiff Douglas has made purchases at a Home Depot store in Illinois repeatedly during the summer of 2019.

48. When Plaintiff Douglas entered the Home Depot stores, he was repeatedly viewed by Home Depot's security cameras, which captured and collected Plaintiff Douglas's faceprint. In fact, Home Depot has collected a new faceprint from Plaintiff Douglas each time he appeared on a different security camera, meaning several times per store visit.

49. Home Depot shared the security-camera footage and Plaintiff Douglas's faceprint with Defendant Doe.

50. Defendants do not provide a publicly available retention schedule specifying the period for which they will retain Plaintiff Douglas's faceprint.

51. Defendants have never informed Plaintiff Douglas of the purpose for which they were capturing or collecting his faceprint or the duration for which they

would retain it, nor did Defendants receive a written release from Plaintiff Douglas authorizing the collection.

52. Because he was never informed of the collection of his faceprint, Plaintiff Douglas did not consent to the capture or collection of his faceprint.

53. Plaintiff Douglas was injured as a result of the violation of his legally protected right not to have his faceprint collected without consent.

#### **FACTUAL ALLEGATIONS SPECIFIC TO PLAINTIFF YOUNG**

54. Plaintiff Young made purchases at a Home Depot store in Illinois in August 2018 and February 2019.

55. When Plaintiff Young entered the Home Depot store, he was repeatedly viewed by Home Depot's security cameras, which captured and collected Plaintiff Young's faceprint. In fact, Home Depot has collected a new faceprint from Plaintiff Young each time he appeared on a different security camera, meaning several times per store visit.

56. Home Depot shared the security-camera footage and Plaintiff Young's faceprint with Defendant Doe.

57. Defendants do not provide a publicly available retention schedule specifying the period for which they would retain Plaintiff Young's faceprint.

58. Defendants have never informed Plaintiff Young of the purpose for which they were capturing or collecting his faceprint or the duration for which they would retain it, nor did Defendants receive a written release from Plaintiff Young authorizing the collection.

59. Because he was never informed of the collection of his faceprint, Plaintiff Young did not consent to the capture or collection of his faceprint.

60. Plaintiff Young was injured as a result of the violation of his legally protected right not to have his faceprint collected without consent.

### **CLASS ACTION ALLEGATIONS**

61. Plaintiffs bring this action pursuant to Fed. R. Civ. P. 23(b)(3) on behalf of themselves and the following class and subclass (collectively, the “Class”):

**Home Depot Class:** All individuals who had their faceprints collected, captured, received, or otherwise obtained while visiting a Home Depot store in Illinois.

**Purchaser Subclass:** All Home Depot Class members who made a purchase at a Home Depot store after Defendants implemented their facial-recognition program.

The following people are excluded from the Class: (1) any Judge or Magistrate presiding over this action and members of their families; (2)

Defendants, Defendants' subsidiaries, parents, successors, predecessors, and any entity in which the Defendants or their parents have a controlling interest and their current or former employees, officers, and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiffs' counsel and Defendants' counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

62. **Numerosity:** The exact number of Class members is unknown to Plaintiffs at this time, but it is clear that individual joinder is impracticable. Defendants have collected, captured, received, or otherwise obtained biometric identifiers or biometric information from hundreds of thousands, if not millions, of individuals within the Class definition, and with damages of at least \$1,000 per violation, the Class easily exceeds the \$5,000,000.00 jurisdictional threshold under 28 U.S.C. § 1332(d). Members of the Class can be identified through Defendants' records.

63. **Commonality and Predominance:** Questions of law and fact common to the claims of Plaintiffs and the Class predominate over any questions that may affect individual members. Those common questions include:

- a. Whether Defendants collected or captured the Class members' biometric identifiers or information;
- b. Whether Defendants maintained a publicly available retention schedule for biometric identifiers or information;
- c. Whether Defendants informed the Class members that they would collect or capture the Class members' biometric identifiers or information;
- d. Whether Defendants informed the Class members of the purpose for which they would collect their biometric identifiers or information, or the duration for which they would retain that data;
- e. Whether Defendants obtained the written release required by BIPA to collect or capture, use, and store the Class members' biometric identifiers or information; and
- f. Whether Defendant Doe profited from the Class members' biometric identifiers or information.

64. **Typicality:** Plaintiffs' claims are typical of the claims of the other members of the Class. Plaintiffs and the Class suffered invasions of privacy as a result of Defendants' uniform wrongful conduct.

65. **Adequate Representation:** Plaintiffs will fairly and adequately represent and protect the interests of the Class and has retained competent counsel experienced in complex litigation and class actions under BIPA specifically.

Plaintiffs have no interests antagonistic to those of the Class, and Defendant has no defenses unique to Plaintiffs. Plaintiffs and their counsel are committed to

vigorously prosecuting this action on behalf of the Class members and have the resources to do so.

66. **Superiority:** This class action is appropriate for certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy, and joinder of the Class members is otherwise impracticable. The damages suffered by the individual Class members are small relative to the burden and cost of individual litigation, and individual litigation is therefore infeasible. Even if Class members could sustain individual litigation, it would increase the delay and expense to all parties relative to a class action because of the complex factual issues raised by the Complaint. A class action presents fewer manageability difficulties and provides economies of scale and uniformity of decisions.

67. Plaintiffs reserve the right to revise the foregoing class allegations and definitions based on facts learned and legal developments following additional investigation, discovery, or otherwise.

**FIRST CAUSE OF ACTION**  
**Violation of 740 ILCS 14/15**  
**Against All Defendants**  
**On Behalf of Plaintiffs, the Home Depot Class, and the Purchaser Subclass**

68. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

69. Home Depot is a Delaware corporation and is therefore a “private entity” under 740 ILCS 14/10.

70. Defendant Doe is either an individual or a partnership, corporation, or limited liability company. Defendant Doe is not a State or local government agency, court of Illinois, clerk of the court, or judge or justice thereof. Defendant Doe is, therefore, “private entities” under 740 ILCS 14/10.

71. When Plaintiffs and the Class members entered Home Depot stores, Defendants used the Home Depot security-camera systems to create faceprints of Plaintiffs and the Class members. Those faceprints mapped the geometry of Plaintiffs’ and the Class members’ faces, and Defendants used that geometry to identify them as they moved through the store, returned to the store, and visited other stores. Defendants therefore collected, captured, received through trade, or otherwise obtained Plaintiffs’ and the Class members’ biometric identifiers and biometric information.

72. Prior to collecting, capturing, receiving through trade, or otherwise obtaining Plaintiffs' and the Class members' biometric identifiers and biometric information, Defendants did not inform Plaintiffs or the Class members or their legally authorized representatives that their biometric identifiers and information would be collected or stored.

73. Prior to collecting, capturing, receiving through trade, or otherwise obtaining Plaintiffs' and the Class members' biometric identifiers and biometric information, Defendants did not inform Plaintiff or the Class members or their legally authorized representatives of the specific purpose and length of term for which their biometric identifiers and information were being collected, stored, and used.

74. Prior to collecting, capturing, receiving through trade, or otherwise obtaining Plaintiff and the Class members' biometric identifiers and biometric information, Defendants did not receive a written release from Plaintiffs and the Class members or their legally authorized representatives authorizing the collection, capture, receipt through trade, or other obtainment and use of their biometric identifiers or information.

75. Plaintiffs and the Class members did not consent to the disclosure or dissemination of their biometric identifiers and information before Home Depot shared their faceprints with Defendant Doe.

76. Home Depot's disclosure and dissemination of Plaintiffs' and the Class members' biometric identifiers and information did not complete a financial transaction requested or authorized by Plaintiffs and the Class members.

77. Home Depot's disclosure and dissemination of Plaintiffs' and the Class members' biometric identifiers and information was not required by State or federal law or municipal ordinance.

78. Home Depot's disclosure and dissemination of Plaintiffs' and the Class members' biometric identifiers and information was not required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction

79. By capturing and collecting, storing, using, and disclosing Plaintiffs' and the Class members' biometric identifiers and information as described herein, Defendants violated Plaintiffs' and the Class members' rights to privacy and property in their biometric data under BIPA.

80. On behalf of themselves and the Class, and pursuant to 740 ILCS 14/20, Plaintiffs seek: (1) injunctive relief requiring Defendants to stop their

unlawful practices and destroy the data unlawfully obtained; (2) liquidated damages of \$5,000 per violation for Defendants' intentional and/or reckless violations of BIPA, or, in the event the Court finds those violations to be negligent, liquidated damages of \$1,000 per violation; and (3) reasonable attorneys' fees and costs.

### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs, on behalf of themselves and the Class, respectfully request that this Court enter an order:

A. Certifying this case as a class action on behalf of the Class and Subclass defined above, appointing Plaintiffs as representatives of the Class and Subclass, and appointing their lawyers as Class Counsel;

B. Declaring that Defendants' actions, as described above, violate 740 ILCS 14/15;

C. Awarding liquidated damages under 740 ILCS 14/20 of \$5,000 per violation for Defendants' intentional and/or reckless violations of BIPA, or, alternatively, liquidated damages of \$1,000 per violation if the Court finds that Defendants' violations were negligent;

D. Awarding injunctive and other equitable relief as necessary to protect the Class, including an order requiring Defendants to stop their unlawful collection of biometric data and to delete any such data that was unlawfully obtained;

E. Awarding Plaintiffs and the Class their reasonable litigation expenses and attorneys' fees;

F. Awarding Plaintiffs and the Class pre- and post-judgment interest; and

G. Awarding such other and further relief as equity and justice may require.

### **JURY TRIAL**

Plaintiffs demand a trial by jury for all issues so triable.

Date: September 4, 2019

**GLORIA BRUNSON, KEVIN  
DAHLBERG, JAMAL DOUGLAS, and  
EARL YOUNG**, individually and on  
behalf of all others similarly situated,

s/ David C. Sawyer

One of Plaintiffs' Attorneys

David C. Sawyer

dsawyer@grsmb.com

Georgia Bar No. 751032

GRAY, RUST, ST. AMAND, MOFFETT &  
BRIESKE, L.L.P.

1700 Salesforce Tower Atlanta

950 East Paces Ferry Road  
Atlanta, Georgia 30326  
(404) 870-7439

Ashley C. Keller\*  
ack@kellerlenkner.com  
Travis D. Lenkner\*  
tdl@kellerlenkner.com  
J. Dominick Larry\*  
nl@kellerlenkner.com  
KELLER LENKNER LLC  
150 N. Riverside Plaza, Suite 4270  
Chicago, Illinois, 60606  
(312) 741-5220

Warren D. Postman\*  
wdp@kellerlenkner.com  
KELLER LENKNER LLC  
1300 I Street, N.W., Suite 400E  
Washington, D.C. 20005  
(202) 749-8334

*\*pro hac vice* to be sought

*Counsel for Plaintiffs and the Putative  
Class*

**IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF GEORGIA  
ATLANTA DIVISION**

GLORIA BRUNSON, KEVIN  
DAHLBERG, JAMAL DOUGLAS,  
and EARL YOUNG, individually and  
on behalf of all others similarly  
situated,

Plaintiffs,

v.

THE HOME DEPOT, INC., Delaware  
Corporation, and JOHN DOE,

Defendants.

Case No.

**COMPLAINT - CLASS ACTION  
AND DEMAND FOR JURY TRIAL**

**LR 7.1(D) CERTIFICATE OF FONT COMPLIANCE**

I hereby certify that the foregoing has been prepared with one of the font and point selections approved by the Court in Local Rule 5.1(C), Northern District of Georgia, specifically Times New Roman 14 point.

Date: September 4, 2019

**GLORIA BRUNSON, KEVIN  
DAHLBERG, JAMAL DOUGLAS, and  
EARL YOUNG**, individually and on  
behalf of all others similarly situated,

s/ David C. Sawyer

One of Plaintiffs' Attorneys

David C. Sawyer  
dsawyer@grsmb.com  
Georgia Bar No. 751032  
GRAY, RUST, ST. AMAND, MOFFETT &  
BRIESKE, L.L.P.  
1700 Salesforce Tower Atlanta  
950 East Paces Ferry Road  
Atlanta, Georgia 30326  
(404) 870-7439

Ashley C. Keller\*  
ack@kellerlenkner.com  
Travis D. Lenkner\*  
tdl@kellerlenkner.com  
J. Dominick Larry\*  
nl@kellerlenkner.com  
KELLER LENKNER LLC  
150 N. Riverside Plaza, Suite 4270  
Chicago, Illinois, 60606  
(312) 741-5220

Warren D. Postman\*  
wdp@kellerlenkner.com  
KELLER LENKNER LLC  
1300 I Street, N.W., Suite 400E  
Washington, D.C. 20005  
(202) 749-8334

*\*pro hac vice* to be sought

*Counsel for Plaintiffs and the Putative  
Class*